Privacy Impact Assessment
for the

PRISM System

June 4, 2009

Contact Point
Greg Naylor
DHS/Management/OCPO/Oversight and Strategic Support/Acquisition Systems Branch
(202) 447-5325

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Department of Homeland Security (DHS) Management Directorate, Office of the Chief Procurement Officer (OCPO) is the owner of the PRISM contract writing management system. PRISM provides comprehensive, Federal Acquisition Regulation (FAR) based acquisition support for all DHS headquarters entities. The purpose of this Privacy Impact Assessment (PIA) is to document how PRISM collects, uses, disseminates, and maintains personally identifiable information (PII).

Overview

The DHS Management Directorate, OCPO, is responsible for awarding and administering contracts and purchase orders to support the DHS mission, goals and objectives. OCPO provides vital procurement and logistic services to DHS components, support offices, and leadership in applying fundamentally sound business practices to the Department's acquisition of goods and services. The OCPO is the owner the PRISM contract writing management system. PRISM is a Commercial-off-the-Shelf (COTS) software product that provides full procurement life-cycle support including all phases from advanced acquisition planning through contract closeout. PRISM provides procurement/acquisition support at the desktop through a browser only, giving global access to all DHS procurement personnel and their customers. OCPO staff also access PRISM to obtain procurement data reports.

Procurement Actions

PRISM provides development, processing, and management functionality for the following procurement actions, excluding purchase card transactions:

- Procurement requisitions - documentation of an agency’s need for supplies or services to include the description of requirements to satisfy agency needs and certification of funding availability.

- Solicitations - any request to submit offers or quotations to the Government. Solicitations under sealed bid procedures are called “invitations for bids.” *Solicitations* under negotiated procedures are called “requests for proposals.” Solicitations under simplified acquisition procedures may require submission of either a quotation or an offer.

- Contracts - a mutually binding legal relationship obligating the seller to furnish the supplies or services (including construction) and the buyer to pay for them. It includes all types of commitments that obligate the Government to an expenditure of appropriated funds and that, except as otherwise authorized, are in writing. In addition to bilateral instruments, contracts include (but are not limited to) awards and notices of awards; job orders or task letters issued under basic ordering agreements; letter contracts; orders, such as purchase orders, under which the contract becomes effective by written acceptance or performance; and bilateral contract modifications. It includes, among other things:

- Simplified acquisitions - the acquisition of supplies and services, including construction, research and development, and commercial items, in which the aggregate amount does not exceed the simplified acquisition threshold, generally $100,000.

- Interagency agreements - a procedure by which an agency needing supplies or services (the requesting agency) obtains them from another agency (the servicing agency). Often through the servicing agency's acquisition of the supply or service from the private sector

- Blanket purchase agreements - a simplified method of filling anticipated repetitive needs for supplies or services by establishing charge accounts with qualified sources of supply.

- Basic ordering agreements - a written instrument of understanding, negotiated between an agency, contracting activity, or contracting office and a contractor, that contains terms and clauses applying to future orders between the parties during its term; a description, as specific as practicable, of supplies or services to be provided; and methods for pricing, issuing, and delivering future orders under the basic ordering agreement.

PRISM includes tools that enhance and support requirements generation, approval, workflow processing, and other steps of the procurement process, including closeout.

Tools and Uses

Within PRISM, information flow includes the creation of procurement packages within a user interface provided and controlled by PRISM. Documents are created and uploaded with the use of forms and data entry fields; data entry is limited to what is allowed in each data entry field. Where users upload documents, these are strictly stored by PRISM and are not processed or acted on by the software. Procurement packages and documents can be viewed, checked out, and printed by authorized users. PRISM can also be used for generating reports. DHS regularly transmits information to two non-DHS systems; the Federal Procurement Data System – Next Generation (FPDS-NG) and FedConnect.

FPDS-NG is a publically available database that contains procurement transaction information. PRISM electronically transmits information that does not contain personally identifiable or proprietary information to FPDS-NG. This information includes but is not limited to agency identifier, procurement document number, award and expiration dates.

FedConnect is a full-service web portal, hosted by the vendor Compusearch, which allows DHS to post acquisition opportunities to a central location where vendors can search the opportunities, submit responses, and receive awards. DHS transmits solicitation and supporting data to FedConnect for bid and proposal receipt purposes. PII that is transmitted to FedConnect is limited to Government contact information to allow communication between potential vendors and DHS.

Typical Transaction

A typical transaction in PRISM starts with the communication of user requirements in the form of a requisition or purchase request provided by the program office. A contract specialist can then use a variety of competitive methods to develop solutions to satisfy the requirements. A warranted contracting officer will review the work of the contract specialist, and when appropriate, award a contract. Because DHS has no interface to the financial system, a copy of the award document is printed and sent to the finance office for obligation and payment purposes.

Section 1.0
Characterization of the Information

1.1 What information is collected, used, disseminated, or maintained in the system?

The PII collected consists of data elements about DHS authorized users and vendor points of contact. PII maintained in the system for DHS authorized personnel is limited to the following information:

- Full name;
- Work telephone number; and
- Work e-mail address;

The PII for vendors is as follows:

- Vendor contact full name;
- Vendor contact work telephone number;
- Vendor contact work e-mail address; and
- Also, if necessary, full name of key personnel in a vendor proposal.

1.2 What are the sources of the information in the system?

PRISM collects information directly from DHS employees, DHS contractor employees, the Central Contractor Registration[1] (CCR) database, and vendors. DHS employees and contractor employees requiring access to PRISM must provide the requisite information in order to gain access to the system. Vendors responding to DHS solicitations often provide proposals or other data, which may contain PII, Taxpayer Identification Numbers (TINs), and contact information transmitted to PRISM, which are stored as attachments.

[1] Central Contractor Registration (CCR) is the primary registrant database for the U.S. Federal Government. CCR collects, validates, stores and disseminates data in support of agency acquisition missions. Both current and potential federal government registrants are required to register in CCR in order to be awarded contracts by the federal government. CCR validates the registrant information and electronically shares the secure and encrypted data with the federal agencies' finance offices to facilitate paperless payments through electronic funds transfer (EFT). Additionally, CCR shares the data with federal government procurement and electronic business systems.

1.3 Why is the information being collected, used, disseminated, or maintained?

PRISM collects information to manage the acquisition process for the procurement of services and supplies. More specifically, information collected from DHS authorized users is necessary to establish accountability and to track workload related processes concerning procurement transactions.

Information collected from DHS vendors is required by the FAR and necessary to accurately document, award, and manage procurement actions, including ensuring that vendors are properly compensated for goods delivered or services performed. Since October 1, 2003, FAR, Subpart 4.11 mandates that vendors wishing to do business with the federal government must be registered in CCR before being awarded a contract. Limited exceptions apply. FAR requires that vendor information be included in contracts. PRISM is the contract writing system mandated for use in DHS.

1.4 How is the information collected?

PRISM collects information directly from DHS employees. If a new end user account is needed, the end user completes a User Account Request form, has their government supervisor/point of contact sign, and provides it to the Principal Site Administrator (PSA) via fax, e-mail or hand delivery.

Most vendor information is pre-loaded into PRISM via electronic download of CCR data on a monthly basis through a secure procedure where a DHS database administrator logs into the secure CCR website using the DHS agency user ID and password and downloads the complete vendor file. The batch file is then uploaded to the PRISM application, which requires a PRISM user ID and password. Daily updates are made through the same secure procedure as needed. In some cases, the requisitioner, contract specialist or contracting officer may manually enter information into the PRISM system. Vendors submit proposals as part of the procurement process which may contain PII that is necessary for proposal evaluation or contract management.

1.5 How will the information be checked for accuracy?

PRISM collects information directly from DHS personnel via the User Account Request form provided to the PSA for processing. The PSAs are responsible for verifying that each employee requesting a PRISM account has the appropriate clearance. Employees will only be granted access if they have an approved security clearance from DHS. The PSAs are responsible for verifying that each employee requesting a PRISM account has the appropriate clearance. Each end user must sign the acknowledgement of the rules of behavior when requesting a new account.

PRISM collects vendor information mainly from CCR. The PII from the CCR is deemed reliable since the vendor supplies and maintains it directly. Other PII can be supplied by the vendor as part of a proposal that is necessary for proposal evaluation or contract management. Business rules also require that the contract specialist and contracting officer verify the vendor information as part of the contract award process.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The department's organic legislation presupposes the acquisition of goods and services to accomplish its mission. 6 U.S.C. §§112(b), 341; 6 U.S.C. ch. 1, subch. VIII, pt D. PRISM is the tool employed by DHS to track, manage, and report on procurement transactions which requires limited employee and vendor PII in order to accomplish those tasks.

FAR Subpart 4.1102, Policy, requires that prospective contractors be registered in the CCR database prior to award of a contract or agreement, which authorizes the use of limited vendor PII as contained in the CCR system.

The Electronic Funds Transfer (EFT) Act requires that most federal payments be made electronically. As a result, any vendor of the Federal government is required to receive payment by EFT which authorizes use of vendor TIN, which may be associated with an individual and is obtained from the CCR.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

There is a threat to privacy of information being electronically intercepted by an unauthorized individual. To counter this threat, remote access to PRISM is not allowed. Authorized DHS users may only access PRISM from within the secure DHS environment, which is strictly controlled, and must possess a valid user account and password.

Also, there is a privacy risk of the data downloaded from the CCR being electronically intercepted by an unauthorized individual. This risk is mitigated by making a Secure Sockets Layer (SSL) connection to the secure CCR File Transport Protocol website to download the extract.

Section 2.0 Uses of the Information

2.1 Describe all the uses of information.

PRISM uses data to accomplish all stages of acquisition from requirements gathering to contract closeout, workload management and reporting. Internally, PRISM can use information to create requisitions, solicitations, award documents supporting simplified acquisition and large contract procedures per the FAR, contract modification documents, interagency agreements, blanket purchase agreements, and basic ordering agreements. Additionally, PRISM uses information to internally manage the acquisition process by establishing user accounts and tracking workload related processes on procurement transactions. Reports are generated to track and help manage program area workload, provide information in support of DHS procurement goals and objectives, as well as managing the PRISM system itself.

Externally, PRISM transmits select PRISM information to FPDS-NG to satisfy FAR reporting requirements. It is a requirement for PRISM to report awarded and executed procurement transactions that meet specific guidelines and thresholds. Federal contract data at FPDS-NG is available to all federal agencies, Congress, the Office of Management and Budget, and the general public. No PII or proprietary information is transmitted to FPDS-NG. DHS also transmits solicitation and supporting data to FedConnect including Government contact information to allow bi-directional communication between DHS and potential vendors.

OCPO confirms and loads basic DHS user information into PRISM in order to manage access. It also uses vendor PII in the solicitation, evaluation, award, and contract administration efforts of the acquisition process.

2.2 What types of tools are used to analyze data and what type of data may be produced?

PRISM has a complete reporting function for several different user types. These reports are generated for analysis by DHS staff as well as auditors. These reports have the capability of identifying procurement transactions with individual procurement personnel. Access to the reporting function is controlled through roles.

PRISM also interfaces with FPDS-NG, which is a publicly available database. The data transmitted to FPDS-NG from PRISM is restricted to information related to the procurement transaction. Primary data regarding the awarded action itself such as agency identifier, procurement document number, award and expiration dates, contract type, value, obligation, and description are transmitted. Other explanatory data items regarding the transaction are also provided to FPDS-NG; such as whether it is an item of National Interest, place of performance, Product Service Code, North American Industry Classification System (NAICS) code; competitive data (e.g. extent competed, type of set-aside, solicitation procedures used), as well as contracting officers business size determination. PRISM electronically transmits information that does not contain personally identifiable or proprietary information to FPDS-NG. FPDS-NG is a public data source that anyone can access.

Crystal Reports is a COTS software package that can also be used to generate internal reports against the PRISM database. Crystal Reports is loaded on select individual computer desktops. Some users who have Crystal Reports also use SQL plus to run queries. Users of these tools have read only accounts to connect to the database. Access to the database for Crystal Reports and SQL plus is controlled through firewall access and read only database accounts.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

PRISM obtains vendor data from the CCR. The CCR is the primary registrant database for the U.S. Federal Government. CCR collects, validates, stores, and disseminates data in support of agency acquisition missions, including Federal agency contract and assistance awards and is searchable by the general public.

Both current and potential federal government registrants are required to register in CCR in order to be awarded contracts by the federal government. Registrants are required to complete a one-time registration to provide basic information relevant to procurement and financial transactions. Registrants must update or renew their registration at least once per year to maintain an active status. Certain PII CCR data that is generally available to Government users is also publicly available through the internet at the election of the vendor, including, potentially: contact names for business, electronic business and past performance information on the firm, including business addresses and phone numbers.

CCR validates the registrant information and electronically shares the secure and encrypted data with the federal agencies' finance offices to facilitate paperless payments through EFT. Additionally, CCR shares the data with federal government procurement and electronic business systems.

PRISM uses the data from CCR to comply with federal regulations that require use of the CCR for contract writing and procurement tracking systems. The data is stored in PRISM and when vendors are selected, the data is pulled from the CCR data to populate DHS records with the contractor supplied data. This data is required to award and administer contracts and simplified acquisitions on behalf of the Department. The information collected also allows DHS to comply with federally mandated reporting requirements to FPDS-NG, Freedom of Information Act requests, and inquiries from Congress.

Access within PRISM to data from the CCR is controlled by defined roles. Only a limited set of roles can view data such as the TIN, which in some instances could be PII.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

There is a risk of using information in PRISM for reasons outside of its original collection. To mitigate this risk access to the PRISM system requires account credentials and a password. All users have received DHS Security training and PRISM training prior to being granted access to production systems. Access to PRISM is limited to the minimum access needed to perform their respective functions based on roles, sites, and security groups. This allows users to perform appropriate duties in the system for which they have responsibility and prevents users from seeing more information than they are required in order to do their jobs. Changes to user accounts are tracked and audited through the use of transaction history tracking which provides information on data changes made and the specific user who made the change.

Each system user must possess the appropriate need to know as well as a qualified job position with procurement responsibilities in order to receive a user account and also must complete the Rules of Behavior. The PRISM user audience does not include members of the general public.

Changes to contract documentation are handled through modifications and are governed through federal regulation included in the FAR.

Section 3.0 Retention

3.1 How long is information retained?

Procurement data is retained for the life of the contractual action, plus a specified period of time after the action has been completed. The procedures and retention periods for contract files and data is set forth in section 4.805 of the FAR and General Records Schedules (no. 3) published by the National Archives and Records Administration. These procedures and schedules take into account documents created and held in electronic media within PRISM. Retention periods of data for contract information vary according to context and circumstance, but, with respect to completed contract files, disposal customarily occurs 6 years and 3 months after final payment.

User accounts are retained for the life of the system. Users who no longer require a PRISM account cannot be deleted from the system, however, the login rights are removed from the account and it is then deactivated. Deletion of user accounts would eliminate pertinent historical elements of the procurement records.

3.2 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

Procurement data retention is prescribed by the FAR and consistent with DHS Records Management Handbook, MD 0550.1, January 2007 and General Records Schedule 3 issued by NARA.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

PRISM collects only the DHS authorized user and vendor PII information required to properly track, record, and manage acquisition efforts of the Department to comply with the FAR requirements. Records will be retained to comply with DHS policy as well as federal regulation requirements.

There is a risk that retained PII may become accessible if not securely stored. This risk is mitigated by the fact that PII stored in the system is protected by rule-based access controls for roles, sites, and security groups. PII contact data that becomes part of the contract is only visible in the system to authorized personnel. In addition, data retention policies are in accordance with FAR regulations.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Within DHS the Office of the Chief Procurement Officer (OCPO), Immigration and Customs Enforcement (ICE), and Citizenship and Immigration Services (CIS) share one instance of PRISM. Access to other component sites are controlled through role-based and site-based access, as well as the use of security groups within PRISM preventing unauthorized sharing of information. The full content of each procurement record is visible to a limited number of authorized contracting staff across component sites. This allows for contract data reuse, sharing of contracts, and information sharing on a need-to-know basis. This shared access allows DHS components to take advantage of similar or identical procurement actions already in existence minimizing duplication of efforts which saves time and administrative cost.

Vendor TINs are shared with the Office of the Chief Financial Officer (OCFO) for payment purposes. The TINs are provided to the proper OCFO personnel manually. No electronic interface currently exists between PRISM and any financial system. No PRISM user account information is disclosed or shared internally or externally.

Data from the PRISM system can be used to fulfill data requests from the DHS Inspector General (DHS IG). The dissemination of PII in these instances is generally not required. However, were PII to be specifically requested, it would be processed at a higher management level for approval prior to dissemination.

4.2 How is the information transmitted or disclosed?

OPO, ICE, and CIS share one instance of PRISM, meaning procurement actions from all three components reside in the same database, and therefore data does not need to be transmitted to be shared. Access across sites is limited and controlled through role-based and site-based access, as well as the use of security groups. These safeguards prevent unauthorized sharing of information within PRISM. Some contract information is viewable by contracting staff across components in order to minimize redundancy and reduce costs.

Data sets from PRISM are provided to the DHS IG, whether PII or not, are only provided as requested and provided either in hard copy or electronically outside of the PRISM environment (e.g. e-mail). Any information (whether it is PII or not) shared with DHS IG is required to be properly secured.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Electronic procurement information for OCPO, ICE, and CIS is maintained within a central, secured database. Procurement records for each component are segmented by separate sites within PRISM. Access to all data within PRISM, including PII, could represent a privacy risk. To mitigate this risk, general PRISM access is controlled through the use of system ID and password. System access is granted on a valid "need-to-know" basis that is determined by the users assigned duties and intended system usage, as well as supervisory approval. Access across sites is further controlled through role-based and site-based access, as well as the use of security groups. These controls prevent unauthorized sharing of information without a "need-to-know." Access to the security functions (e.g., audit trails, access control lists, and password files) is restricted to system administrators and database administrators. All change activity associated with security settings is recorded in an audit log.

Any information transmitted to the DHS IG would be in response to a formal request for the data and would be documented in a correspondence tracking system audit trail. To mitigate an inadvertent release of PII, DHS IG does not have access to the information stored in PRISM (other than non-PII transmitted to FPDS-NG) unless that information is included in official correspondence to or from DHS; is related to the inquiry; or involves an official response by DHS to the inquiry.

Section 5.0 External Sharing and Disclosure

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

All contract actions are made public through the FPDS-NG. PII is not shared with FPDS-NG.

PRISM transmits solicitation and supporting data electronically to FedConnect as part of the pre-award process. PRISM also transmits contractual data electronically to the FPDS-NG as part of the contract award process. FAR Part 4.602 requires Federal agencies to report acquisition activities to the FPDS-NG. These secure transmissions are a function within PRISM.

Data from the PRISM system can be used to fulfill data inquiries from Congress, General Accountability Office (GAO), and Freedom of Information Act (FOIA) requests. The dissemination of PII in these instances would not generally be permitted. However, if an inquiry would request PII data, it shall be processed at a higher management level for approval prior to dissemination.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

Other than contact information, PII within PRISM is not generally collected with the intent to share it outside the Department. PII may be shared in instances such as inquiries by the GAO under the General Information Technology Access Account Records System (GITAARS) [DHS/ALL-004, May 15, 2008, 73 FR 28139] and the Department of Homeland Security Contractors and Consultants [DHS/ALL-021 October 23, 2008, 73 FR 63179] SORN.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Contract information is uploaded from PRISM through a secure and encrypted connection to FPDS-NG. Preaward information is uploaded from PRISM through a secure and encrypted connection to FedConnect. The DHS instance of PRISM employs FIPS 140-2 and/or DHS policy compliant SSL encryption for security of client-to-server communications over SSL user sessions. In this manner strong security encryption is used to prevent eavesdropping of communications where traffic may be passing over insecure networks. The Data Universal Numbering System (DUNS) number is passed to FPDS-NG as the unique, key identifier to retrieve vendor information directly from the CCR to FPDS-NG. The DUNS is not considered PII.

Any PRISM information provided to the GAO, whether PII or not, is only the minimum required data and is provided either in hardcopy or electronically outside of the PRISM environment (i.e. e-mail). Any information (whether it is PII or not) shared with agencies outside of DHS is required to be properly secured by the receiving organization.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

The privacy risk related to external sharing of data with FPDS-NG and FedConnect is minimal since PRISM does not share PII externally with FPDS-NG and only transmits DHS contact information to FedConnect through the PRISM environment. Risk is mitigated by only allowing minimal PII to be transmitted and it is done so through secure transmissions to FedConnect.

Any information transmitted to the GAO or for FOIA purposes would be in response to a formal request for the data and would be documented in a correspondence tracking system audit trail. To mitigate an inadvertent release of PII, the GAO and the public do not have access to the information stored in PRISM (other than non-PII transmitted to FPDS-NG) unless that information is included in official correspondence to or from DHS; is related to the inquiry by that agency; or involves an official response by DHS to the inquiring agency.

Section 6.0 Notice

6.1 Was notice provided to the individual prior to collection of information?

PRISM does not collect information without the user's knowledge or consent. The collection of information from a DHS authorized user is not made prior to them receiving the PRISM User Account Request and Rules of Behavior forms. A Privacy Act Statement is included as part of the PRISM User Account Request form. Notice is also provided to employees by the General Information Technology Access Account Records System (GITAARS) DHS/ALL-004, May 15, 2008, 73 FR 28139 System of Record Notice (SORN).

Vendors who have registered with CCR and provided information through that system are aware that it will be shared by Federal agencies as part of the registration process. Pursuant to the savings clause in the Homeland Security Act of 2002, Public Law 107-296, Section 1512, 116 Stat. 2310 (November 25, 2002), the Department of Homeland Security (DHS) and its components and offices have relied on preexisting Privacy Act systems of records notices for the maintenance of records that concern the Department's accounts payable records. Notice is provided to vendors by the following legacy SORNS: Treasury/CS.207 Reimbursable Assignment/Workticket System (66 FR 52984 October 18, 2001), Treasury/CS.249 Uniform Allowance-Unit Record (66 FR 52984 October 18, 2001), and Treasury/CS.269 Accounts Payable Voucher File (66 FR 52984 October 18, 2001).

6.2 Do individuals have the opportunity and/or right to decline to provide information?

DHS and contractor employees are requested to provide information, limited to their name, work phone and work e-mail address, for PRISM system access. An individual may decline to provide information, however, if certain basic information is not provided, the employee cannot be granted access to the PRISM system. This access is required to effectively manage the acquisition process for services and supplies that will be procured. The data items collected about DHS authorized users is necessary to establish accountability and to track workload related processes concerning procurement transactions.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

No. OCPO only uses the information to perform procurement duties. Individuals may not define particular uses of information. The use of vendor data within contracts is governed by the FAR.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

DHS authorized users and vendors receive notice prior to the time information is collected as stated in section 6.1. PRISM user accounts are not established until the user requesting access has a suitability-clearance and has completed the PRISM User Account Request and Rules of Behavior forms. When a new account is needed, the user or their supervisor will request a User Account Request form from the PSA; typically via phone or e-mail. This form is provided to the requestor via e-mail, fax, or in hard copy. The requestor completes the form and provides it to their government supervisor for acknowledgement and signature, and it is then provided to the PSA.

Most vendors with access to PRISM are versed in FAR regulations and the requirement to provide PII to the CCR for use on federal contracts.

Section 7.0 Access, Redress and Correction

7.1 What are the procedures that allow individuals to gain access to their information?

DHS employees have access to their personal information through the PRISM application. The PII collected for access is necessary in order to create the account and access data within the PRISM system.

Vendor PII is generally controlled by them through the CCR database. A vendor will be given a copy of the award document as part of the contract award process. For PII within the contract document, any changes would require a contract modification for the change to take effect.

7.2 What are the procedures for correcting inaccurate or erroneous information?

DHS employees who have PRISM access are able to change their phone number and e-mail address once they are logged in the system if corrections are required. For changes or corrections to the name or system ID, a system or site administrator's assistance would be required.

Vendors in the PRISM system have the ability to change their PII by making corrections to the data contained in the CCR system. Once they have completed the corrections, these changes will be uploaded in the PRISM system when file updates are retrieved from the CCR. Changes to PII in award documents would require a formal modification be executed.

7.3 How are individuals notified of the procedures for correcting their information?

DHS employees with PRISM access are provided with a Preferences Training Workbook which contains procedures for making changes to their login profile data. However, only system Administrators can change settings for system ID or user name in the PRISM system.

Vendors that require changes to contact data or other privacy information need to do so in the CCR and comply with CCR system requirements in order to make changes to their data. These changes would be initiated and processed outside the control of PRISM. Those changes would then be available to federal agencies when the updated CCR information is downloaded. Changes to the formal contract data, as stated above, would require changes to the award documentation. The changes requested would need to be conveyed to both vendor and government procurement personnel in order to develop and process the required change.

7.4 If no formal redress is provided, what alternatives are available to the individual?

The ability to correct or change PII in the PRISM system is provided to users and vendors. The processes to enact data changes in PRISM are different for DHS employees and vendors and are stated in paragraph 7.2 above.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Very little PII is collected for PRISM user accounts. However, with any manually correctable data, there is a risk that data could be entered incorrectly in the system. Any risk that the individual may not be able to correct their information is mitigated by allowing individuals to access and/or amend most information in their accounts at any time. Individuals may access their information by logging into PRISM directly. In the event that corrections are required that are beyond the control of the user (first/last name and user account ID), a system or site administrator will have to be contacted to make the corrections. Again, there is the risk that PII could be entered incorrectly and this risk is mitigated by allowing individuals to access and/or amend most information in their accounts at any time. Corrections can be made until the data within the user account is correct. In the event that the user ID needs to be corrected, a new user account would be created by copying the existing account and making the necessary corrections to the user ID. The incorrect account ID can not be deleted, but the data within it can be sanitized to remove any PII and then deactivated.

Section 8.0 Technical Access and Security

8.1 What procedures are in place to determine which users may access the system and are they documented?

The process and procedures are documented in the Homeland Security PRISM Administration Manual, dated 04/01/2008. All forms are attached to the manual as well. The process and procedures are as follows:

When a new end user account is needed, end users complete a User Account Request form, have their government supervisor sign and approve the request and provide it to the PSA. Alternatively, this form can be copied into the body of an email and sent from the Supervisor to the PRISM coordinator who would forward it to the PSA. No employee will be granted access to the PRISM application without verifying the employee has an adequate approved security clearance from DHS. Each end user must sign the acknowledgement of the rules when requesting a new account.

The PSA will follow this procedure:

1. Ensure that the user has completed the appropriate PRISM training.
2. Ensure that the user has been cleared for employment at DHS.
3. Once #1 and #2 have been confirmed, the PSA will create the user account.
4. The PSA will notify the user of their ID and temporary password.
5. The PSA will store the User Account Request form and signed acknowledgement of Rules of Behavior.

8.2 Will Department contractors have access to the system?

Contractors will have access to PRISM and will follow the same processes and procedures to gain access to the PRISM application set forth by the Department. They must have a suitability-clearance, and complete the Rules of Behavior and the PRISM User Account Request before an account is created.

DHS suitability-cleared contractors also serve in support rolls to operate and maintain the PRISM system.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

DHS provides the necessary training to all appropriate personnel including privacy and computer security training. No additional training for PRISM is required.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

The DHS PRISM system was established in December 2003. PRISM has completed the C&A process and has an Authorization to Operate (ATO) in accordance with NIST guidelines and DHS Management Directive 4300A. With the relocation of the PRISM instance to the Stennis facility, the PRISM application successfully updated the C&A documentation. The most recent ATO is good for three years and is valid through June, 2011.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

The PRISM System Administrator reviews the PRISM audit log reports weekly. The reports include the login report, user profile change report, system security change report, deletion audit log report, unreleased audit log report, and the release without validations audit log report. The PRISM System Administrator looks for unusual activities that might indicate misuse of the system, such as an excessive number of "release without validation" transactions in a short period of time. The PRISM System Administrator will respond to unusual activity in an appropriate manner through the use of incident reports. An incident report is a notification to the PRISM Information System Security Officer (ISSO). A determination is made as to whether an incident is considered significant in nature or not. If it is considered insignificant, a verbal warning would be appropriate. If the incident is considered significant, the appropriate response would be determined based upon the severity as determined by the ISSO.

Audit and accountability trails maintain a record of system activity by application processes and by user activities. In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification.

Access is controlled through role-based and site-based access as well as the use of security groups within PRISM prevents unauthorized sharing of information. Some contract information is viewable by contracting staff across components. This allows for reuse, sharing of contracts, and information sharing on a need-to-know basis.

Future planned controls for access enforcement include periodic supervisory reviews to ensure user account privileges are being assigned and used appropriately. This will be supported by periodic use of auditing practices and log information. PRISM user groups will be reminded from time to time that user account auditing practices are in place.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

A lack of security procedures and policy in the use of information systems may present a privacy risk. To minimize that risk, all users have received a suitability-clearance, DHS Computer Security training, and PRISM training prior to being granted system access. Access to PRISM also requires a DHS domain account and that the user log on through the secure DHS environment.

There is a risk with PRISM of an authorized individual having more permissions than required to perform their job function. This risk exists when any new user account is created and to counter this risk, each PRISM Site Administrator is responsible for reviewing the permissions to ensure that individual users are only granted the permissions that they are authorized to hold and for which they have a valid need. Access to PRISM is limited to the minimum access needed to perform their respective functions based on roles, sites, and security groups. This allows users to perform appropriate duties in the system for which they have responsibility and prevents users from seeing more information than they are required.

The risk of an unauthorized but cleared DHS employees viewing material on PRISM to which he or she is not authorized to view is mitigated by the use of session locks and process termination routines that will disable access to PRISM after a set period of inactivity. After the session is terminated, the user must establish a new PRISM session using the appropriate identification and authentication procedures.

There is also the risk of unauthorized DHS users trying to access the PRISM system from within the DHS secure environment. To mitigate this risk, to access PRISM as either an administrator or as an end user, individuals must have a valid and active account. Encrypted passwords are stored in the PRISM database, conform to the DHS password complexity rules, and must also be updated every ninety (90) days. System access is denied after three unsuccessful login attempts.

To mitigate the risk of system compromise from external sources, intrusion detection systems are deployed at the enclave boundary and at layered or internal enclave boundaries. Similarly, full audit capability is enabled, including normal system administrator access as well as any unauthorized-user activity. In addition there is a continuous on-line monitoring and audit trail creation capability for all firewalls deployed with the capability to immediately alert proper personnel of any unusual or inappropriate activity.

Electronic eavesdropping of the data while making connections through the Internet could be a privacy risk as well. Risk is mitigated by employing FIPS 140-2 and/or DHS policy compliant SSL encryption for secure communications over SSL user sessions. In this manner strong security encryption is used to prevent eavesdropping of communications where traffic may be passing over insecure networks.

Section 9.0 Technology

9.1 What type of project is the program or system?

The PRISM system is a COTS software product that is in the Operational and Maintenance life cycle phase.

9.2 What stage of development is the system in and what project development lifecycle was used?

PRISM is a mature COTS software product, and as such, DHS did not fund the original development. The DHS instance of PRISM is a web-architected application that required no code customization or modifications for installation, but is tailored for DHS use through built-in switches and configurable business process rules. PRISM has been in use at DHS since December, 2003 and is operational at eight of the nine DHS procurement offices. In accordance with the DHS System Life Cycle process, PRISM is currently in the Operations and Maintenance (Steady State) lifecycle phase. It was declared the official Departmental procurement system prior to the establishment of the Integrated Project Review Team process. It is however counted as part of the Enterprise Architecture portfolio.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

PRISM does not employ any specialized hardware, firmware, or software to gain access. The only client-side software that is required is a standard web-browser; no biometric devices, cameras, RFID or other technology which may increase privacy concerns are employed.

Approval Signature

Original signed copy on file with the DHS Privacy Office.
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security